湖北省中医医院网络安全建设现状分析与思考*

李智一[1,2] 肖 勇[1,2] 沈绍武[1,2]

([1] 湖北中医药大学 武汉 430065 [2] 湖北时珍实验室 武汉 430065)

〔摘要〕 **目的/意义** 分析湖北省中医医院网络安全建设现状，为中医医院网络安全建设提供参考。**方法/过程** 运用统计描述法整体分析中医医院网络安全建设现状，运用卡方检验法以医院级别或信息化投资作为分析维度对比医院网络安全建设现状的差异性。**结果/结论** 湖北省中医医院普遍存在网络安全技术应用不充分、管理制度建设不完善等问题，提出应重视网络安全技术应用、健全管理制度、筑牢数据安全防线等对策建议。

〔关键词〕 网络安全；中医医院；现状分析；湖北省

〔中图分类号〕R-058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673-6036.2024.04.015

Analysis and Considerations on the Current Situation of Network Security Construction in Hubei Traditional Chinese Medicine Hospitals

LI Zhiyi[1,2], *XIAO Yong*[1,2], *SHEN Shaowu*[1,2]

[1] *Hubei University of Chinese Medicine, Wuhan 430065, China*; [2] *Hubei Shizhen Laboratory, Wuhan 430065, China*

〔**Abstract**〕 **Purpose/Significance** To analyze the current situation of network security construction of traditional Chinese medicine (TCM) hospitals in Hubei province, with a view to provide references for network security construction of TCM hospitals. **Method/Process** The statistical description method is used to analyze the current situation of network security construction of TCM hospitals as a whole, and the chi-square test is used to compare the differences of current status of network security construction of hospitals, with the hospital level or information technology investment as the analytical dimensions. **Result/Conclusion** TCM hospitals in Hubei province generally have problems such as inadequate application of network security technology and imperfect construction of security management system. Some countermeasures and suggestions are put forward, such as attaching importance to the application of network security technology, perfecting the management system, strengthening the data security defense line, etc.

〔**Keywords**〕 network security; traditional Chinese medicine hospital; current situation analysis; Hubei province

1 引言

近年来，随着“互联网+”技术在医疗卫生领域的广泛应用，医疗行业正如火如荼开展数字化转型，中医医院不断推进云计算、大数据、人工智能、物联网等技术与医疗服务、医疗管理、患者服务的深度融合应用，互联网医院、线上预约挂号、检查检验结果查看等线上业务与院内医

〔修回日期〕 2023-12-05

〔作者简介〕 李智一，硕士研究生；通信作者：肖勇，教授，硕士生导师。

〔基金项目〕 国家中医药管理局中医药信息化项目（项目编号：GHC-2022-ZFGM-007）；湖北省中医药管理局科研项目（项目编号：ZY2023Q045）。

院信息系统互联互通、信息共享，都给医院网络安全和数据安全带来了风险与挑战。为理清湖北省公立中医医院信息化建设现状，设计“湖北省中医医院信息化建设现状调研表”，基于调查数据系统收集并分析各中医医院网络安全建设现状，剖析存在的主要问题，提出做好网络安全和数据安全的对策建议，旨在为湖北省中医医院网络安全建设工作提供参考。

2 研究对象与方法

2.1 研究对象

数据来源于 2023 年开展的湖北省中医医院信息化建设现状调研。调研获取湖北省 98 家公立中医医院网络安全建设现状数据，其中二级医院 56 家、三级医院 42 家，有效数据 98 份。

2.2 研究内容

主要围绕网络安全技术应用、网络安全管理建设两方面开展研究，其中网络安全技术应用主要包括中心机房安全建设、网络安全技术措施、用户认证模式、数据备份恢复与灾备等；网络安全管理建设主要包括管理制度建立、网络安全等级测评、应急演练等。

2.3 统计方法

使用 Excel 2021 整理汇总湖北省 98 家公立中医医院网络安全建设现状数据，建立专题数据库，使用 SPSS 26.0 软件分析研究数据，应用统计描述方法综合分析中医医院在机房安全、安全技术防护、用户认证、数据备份恢复和灾备以及制度建设、测评实施和应急演练等方面的网络安全现状，应用卡方检验法，以医院级别或信息化投资作为分析维度对比医院网络安全建设现状的差异性。

3 结果

3.1 网络安全技术应用

3.1.1 中心机房安全建设 98 家中医医院均建有中心机房，采用自建模式的达 84 家，占 85.7%；采用其他模式（包括租用云服务、租用场地等）的仅 14 家，占 14.3%。二级、三级医院对比研究表明医院级别对机房建设模式选择无明显影响（$P > 0.05$），见表 1。

表 1 机房建设情况

机房建设情况	二级医院（$n=56$）	三级医院（$n=42$）	χ^2	P
自建	45	39	2.127	0.145
租用（云服务、场地）	11	3		

机房配套设施建设方面，不间断电源（uninterruptible power system，UPS）建设比例最高，防水设备建设比例相对较低，信息化资金投入高于 200 万元的医院，其防水、温湿度监控等设备配套比例较投入不足 200 万元的医院更高，见图 1。

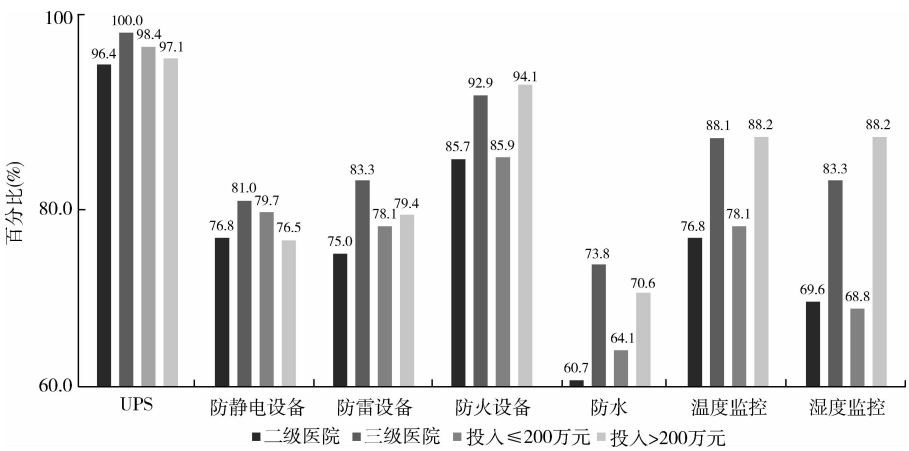

图 1 机房安全配套设施建设情况

3.1.2 网络安全技术防护 96 家中医医院采取了不同程度网络安全措施。综合分析发现，防火墙技术应用比例最高，漏洞扫描、病毒防护、数据备份恢复、权限管理等常见技术应用良好，比例均高于 50%，虚拟专用网络（virtual private network，VPN）、主机安全审计、电子签名等应用比例较低，仅占 30% 左右。对比分析发现，三级医院大多数网络安全措施应用水平高于二级医院，投入高于 200 万元的医院大多数网络安全措施应用水平高于投资不足 200 万元的医院，差异均有统计学意义（$P < 0.05$），见表 2。

表 2 网络安全技术防护措施应用情况

网络安全措施	按医院级别				按信息化资金投入			
	二级医院（$n=56$）	三级医院（$n=42$）	χ^2	P	≤200 万元（$n=64$）	>200 万元（$n=34$）	χ^2	P
防火墙	52	41	0.356	0.551	59	34	2.799	0.160
网闸	14	17	2.658	0.103	15	16	5.729	0.017 *
VPN	14	13	0.426	0.514	14	13	2.977	0.084
网络安全审计	10	19	8.636	0.003 *	11	18	13.623	0.000 *
主机安全审计	10	13	2.291	0.130	10	13	6.320	0.012 *
数据库审计	17	24	7.076	0.008 *	19	22	11.190	0.001 *
日志审计	18	28	11.485	0.001 *	24	22	6.599	0.010 *
漏洞扫描	31	26	0.423	0.516	31	26	7.171	0.007 *
入侵检测	15	21	5.565	0.018 *	17	19	8.213	0.004 *
病毒防护	36	36	5.654	0.017 *	45	27	0.943	0.331
态势感知	8	16	7.357	0.007 *	10	14	7.839	0.005 *
电子签名	12	12	0.662	0.416	12	12	3.286	0.070
单点登录	19	18	0.814	0.367	20	17	3.322	0.068
数据备份与恢复	32	30	2.108	0.147	36	26	3.906	0.048 *
权限管理	37	29	0.097	0.756	38	28	5.331	0.021 *
堡垒机	14	29	18.909	0.000 *	19	24	15.084	0.000 *

注：* 表示 $P<0.05$。

3.1.3 用户认证模式 医院大部分采用了用户名/密码传统认证模式，单点登录、公钥基础设施（public key infrastructure，PKI）数字证书应用比例偏低，动态密码、生物信息识别认证应用比例极低（不足 5%），见图 2。

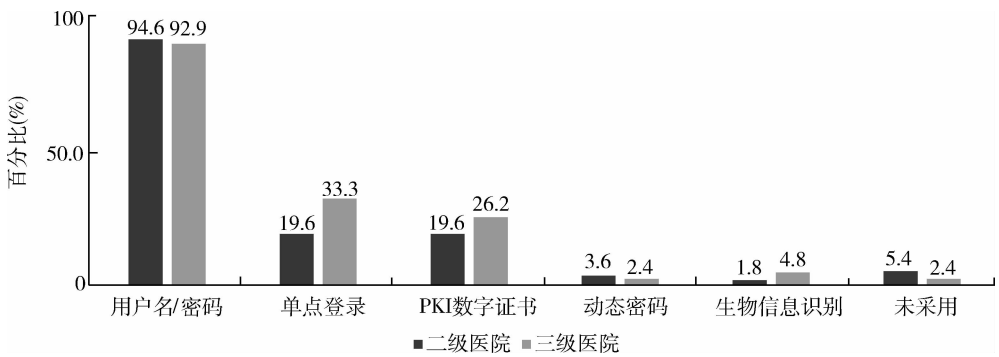

图 2 用户认证模式应用情况

3.1.4 数据备份与恢复 79.6% 的医院具备核心和重点业务系统数据备份能力，数据备份水平整体良好。剔除个别无数据备份的医院，对比分析二、三级医院，其差异无统计学意义（$P>0.05$），医院级别对医院数据备份能力无明显影响。仅 44.9% 的医院具备核心系统数据能恢复到任意时间点且其他

重点业务系统数据能恢复到备份点的能力。相较于数据备份能力，医院数据恢复能力稍显不足。剔除个别无数据恢复能力的医院，对比分析二、三级医院，其差异无统计学意义（$P>0.05$），医院级别对医院数据恢复能力无明显影响。41.8% 的中医医院未建立数据灾备，整体水平偏低。对比分析二、三级医院，其差异无统计学意义（$P>0.05$），医院级别对数据灾备建设无明显影响，见表 3。

表 3 医院数据备份恢复能力情况

	数据备份与恢复能力	二级医院（$n=56$）	三级医院（$n=42$）	χ^2	P
数据备份	全部系统数据备份	22	11	2.655	0.265
	核心和重点业务系统数据备份	22	23		
	仅核心系统数据备份	8	8		
	无数据备份	4	0		
数据恢复	全部系统数据能恢复到任意时间点	14	4	5.499	0.139
	核心系统数据能恢复到任意时间点且其他重点业务系统数据能恢复到备份点	11	15		
	仅核心系统数据能恢复到任意时间点	8	7		
	仅核心系统数据能恢复到备份点	21	16		
	不能恢复	2	0		
灾备方案	无	22	19	3.219	0.359
	有，同楼异处	17	9		
	有，不同楼宇	9	11		
	有，同城异地	8	3		

3.2 网络安全制度建设

3.2.1 网络安全管理制度建立 98 家中医医院中，建立人员安全管理、机房安全管理、网络安全管理、防病毒管理、应急预案管理等制度比例较高（80% 以上），建立信息安全审计管理、系统安全测评管理、安全监控管理等制度比例较低（50% 以下）。二、三级医院对比分析发现，大多数制度建设差异无统计学意义（$P>0.05$），医院级别对网络安全制度建设无明显影响，见表 4。

表 4 医院网络安全管理制度建立情况

网络安全管理制度	二级医院（$n=56$）	三级医院（$n=42$）	χ^2	P
信息安全审计管理	21	21	1.531	0.216
人员安全管理	44	35	0.348	0.555
系统建设管理	25	20	0.086	0.770
系统安全测评管理	17	16	0.643	0.422
机房安全管理	51	37	0.021	0.885
资产管理	21	21	1.531	0.216
介质管理	26	23	0.667	0.414
设备管理	27	26	1.811	0.178
安全监控管理	24	17	0.056	0.813
网络安全管理	44	38	1.695	0.193
系统口令管理	33	29	1.057	0.304
防病毒管理	40	36	2.813	0.093
数据备份与恢复管理	32	36	9.224	0.002*
信息安全事件管理	33	26	0.089	0.766
应急预案管理	49	36	0.067	0.796
以上均未建立	1	0	–	–

注：* 表示 $P<0.05$；– 表示该项不满足卡方检验计算条件。

3.2.2 网络安全测评 44.9% 的中医医院实施了信息系统网络安全等级保护测评。三级医院网络安

全测评实施情况明显优于二级医院，信息化资金投入高于 200 万元的医院测评实施情况明显优于投入不足 200 万元的医院，差异均具有统计学意义（$P<0.05$），见表 5。

表 5 医院网络安全等级测评实施情况

是否实施安全等级测评	按医院级别				按信息化资金投入			
	二级医院（$n=56$）	三级医院（$n=42$）	χ^2	P	≤200 万元（$n=64$）	>200 万元（$n=34$）	χ^2	P
是	18	26	8.593	0.003*	23	21	5.987	0.014*
否	38	16			41	13		

注：* 表示 $P<0.05$。

3.2.3 信息系统故障应急演练 89.3% 的二级医院、所有三级医院均制订了应急预案，组织实施过应急预案演练的二级医院占 66.1%、三级医院占 78.6%。对比研究发现医院级别对应急预案制订与执行情况无明显影响（$P>0.05$），见表 6。71.4% 的医院定期开展至少一项系统故障应急演练，从具体演练项目看，网络故障、业务系统故障应急演练开展比例在 50% 左右，服务器故障应急演练则不足 40%。

表 6 医院应急预案制订与执行情况

应急预案制订与执行	二级医院（$n=56$）	三级医院（$n=42$）	χ^2	P
制订了预案，未开展演练	13	9	5.078	0.077
制订了预案并开展演练	37	33		
未制订预案	6	0		

4 讨论与建议

4.1 讨论

4.1.1 网络安全技术应用不充分 湖北省中医医院在安全计算环境、安全网络环境方面仍需进一步完善，虚拟专用网络、主机安全审计、电子签名应用不足 30%，网闸设备、单点登录应用不足 40%，级别更高或投资水平更高的医院，其网络安全技术措施应用水平明显更高。机房安全建设方面，机房防水设备整体建设比例较低，易产生设备短路风险，但对比湖北省 2018 年调研数据（二级医院达 40% 以上，三级医院达 60% 以上）已有明显进步。用户认证模式方面，超过 90% 的医院仍以用户名/密码的传统认证模式为主，超过 70% 的医院未应用单点登录、电子签名技术，用户终端网络安全防护措施较为单一。数据备份恢复方面，约 80% 的医院开展了核心和重点业务系统数据备份，但不足 50% 的医院能够实现核心系统数据恢复到任意时间点且其他重点业务系统数据恢复到备份点，存在“重备份轻恢复”问题。数据灾备建设方面，41.8% 的医院未实施数据灾备，真正实现有效异地备份的医院仅 30% 左右。

4.1.2 网络安全管理制度不完善 湖北省 50% 以上的中医医院未制订信息安全审计管理、系统建设管理、资产管理、介质管理制度，精细化管理程度不高。网络安全等级测评方面，67.9% 的二级医院、64.1% 的信息化投入不足 200 万元的医院未实施测评，级别更高或投资水平更高的医院，其测评实施情况明显更好。应急预案制订与演练方面，22.4% 的医院制订了应急预案但未开展演练，对比湖北省 2018 年调研数据（48.4% 的中医医院制订了预案但未开展演练）有明显进步；对比中国医院协会信息专业委员会 2021—2022 年度中国医院信息化状况调查报告数据（11.68% 的医院未开展任何应急演练）[1]，湖北省中医医院较全国医院平均水平还有一定差距，具体到各项目指标，湖北省三级中医医院在数据恢复测试、网络故障恢复、服务器故障恢复等方面均低于全国三级医院平均水平。分析发现医院级别或投入水平对湖北省中医医院安全管理制度建设影响不大。

4.2 中医医院网络安全建设措施建议

4.2.1 建立健全网络安全管理体制与运行机制 湖北省中医医院应遵守《网络安全法》《数据安全法》《个人信息保护法》等法律法规，贯彻落实网络安全等级保护管理制度和标准，结合医院建设实际，围绕医院业务应用系统建设、网络安全管理目标及内容范围，研究制定网络安全监控管理、信息安全审计管理、系统建设管理、资产管理、介质管理、数据备份与恢复管理等制度[2]；定期组织信息中心人员、医院职工学习网络安全管理制度、熟悉网络安全法律法规、掌握基本的网络安全防护技术，同时可建立网络安全管理奖惩措施，对制度执行较好的部门或个人予以“网络安全绩效”奖励，激发自觉遵守并落实网络安全管理制度的动力。建立网络安全管理制度执行实施反馈机制，根据实际应用情况及时反馈需要修订的内容，合理科学地调整或新制订相关制度规定。

4.2.2 注重网络安全技术应用与实施 网络安全是动态的而不是静态的。湖北省中医医院应进一步做好中心机房防水、防潮、防雷等防护工作，加大信息化建设资金投入，配置自动消防、自动报警等智能设备，有计划安排相关人员做好出入管理，防止未授权人员随意进入机房[3]。加大虚拟专用网络、网闸设备建设力度，重点加大态势感知、入侵检测、网络安全审计等建设力度，及时分析和处理网络安全风险和威胁，强化网络边界安全。做好网络安全访问控制策略，加强运维审计（堡垒机）建设，集中控制管理内部资源，确保只有授权人员才能访问，防止操作越权行为发生，通过数据库审计、服务器审计等技术手段记录监测其访问操作。强化 PKI 数字证书、单点登录系统建设，实现统一账号管理、统一用户认证、统一权限分配，提高医院信息系统访问安全性与便捷性[4]。

4.2.3 主动实施网络安全等级测评 湖北省中医医院应积极主动实施核心信息系统网络安全等级保护，牢牢把握定级、备案、整改、测评、自查等关键环节，保质保量地做好网络安全等级保护各项工作[5]。定级备案阶段，组织学习网络安全等级保护相关制度和标准，明确网络安全等级保护测评工作的责任和流程。根据不同信息系统应用范围、可用性、保密性要求，合理分类并确定信息系统边界[6]，确定适当的网络安全保护等级并备案。预测评整改阶段，对照网络安全等级保护相关标准进行差距分析，梳理现行系统网络安全现状，按照“就低不就高”的原则，部分符合的绝不判断为符合项，分析研究存在的安全风险和应对举措[7]。预测评与整改应交叉进行，秉持“计划－执行－检查－处理”（plan－do－check－act，PDCA）的持续性改进方法，发现问题立即研究讨论，对可以短时间内整改完成的立即整改，对需要重大改变的列出整改计划表，明确时间节点和任务。

4.2.4 筑牢数据安全防线 湖北省中医医院应研究制订数据采集、传输、储存、分析、报废等全生命周期管理工作规范，建立健全中医临床数据、运营管理数据等的安全监管体系，系统分析医院数据安全所面临的威胁及其存在的脆弱性，评估网络安全与数据安全事件一旦发生可能造成的危害程度，研究提出针对性抵御威胁的防护对策和整改措施，防范和化解医院数据安全风险。采用数据脱敏技术、访问控制技术、存储加密技术、安全审计技术、防勒索技术、防范高级持续性威胁攻击技术等，分类分级保护数据，提供安全的数据查询、复制、使用渠道，促进中医临床数据共享和交换，确保个人隐私和数据安全。破除当前湖北省中医医院存在的“重备份轻恢复”问题，制/修订数据恢复测试管理制度并执行，定期进行数据库恢复演练，确保数据备份的可用性和完整性。有条件的医院可采用“双活＋异地灾备”建设模式，在部署双活数据中心基础上再建立应急容灾数据中心，实现“2＋1”三重保护[8]。按照不同类别的网络安全和数据安全事件，有针对性地研究制订网络安全应急演练方案，多组织开展信息系统应急演练，尽可能模拟网络安全突发事件，及时总结经验并进行反馈整改。

5 结语

随着智慧中医医院的建设与发展，中医医院网

（下转第 102 页）

17 侯丽，康宏宇，钱庆. 医学图书馆公众健康知识服务平台的构建与应用实践［J］. 图书情报知识，2018（2）：40－49，76.
18 BOMHOLD C. Mobile services at academic libraries：meeting the users' needs［J］. Library hi tech，2014，32（2）：336－345.
19 MANOGARAN G，VARATHARAJAN R，LOPEZ D，et al. A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting system［J］. Future generation computer systems，2018（82）：375－387.
20 钱丹丹，许孝君，张丽. 信息生态视域下医学图书馆智慧服务模式构建［J］. 情报科学，2023，41（5）：68－73.
21 翟兴，肖源，王若佳，等. 数智环境下智慧健康信息服务体系构建研究［J］. 情报科学，2022，40（10）：43－50.
22 岳敏敏，董同强. 用户需求导向的高校图书馆健康信息服务研究［J］. 高校图书馆工作，2021，41（5）：55－59.
23 程莹. 英美图书馆公众健康信息服务的实践及其启示［J］. 图书馆界，2020（1）：26－31.
24 邓胜利，付少雄. 美国图书馆的健康信息服务实践及启示［J］. 图书馆杂志，2018，37（11）：76－82.
25 关于促进“互联网 + 医疗健康”发展的意见［EB/OL］.［2023－07－25］. https：//www.gov.cn/zhengce/content/2018－04/28/content_5286645.htm.
26 智慧健康养老产业发展行动计划（2021—2025 年）［EB/OL］.［2023－07－25］. https：//www.gov.cn/zhengce/zhengceku/2021－10/23/content_5644434.htm.
27 数字中国建设整体布局规划［EB/OL］.［2023－07－25］. https：//www.gov.cn/xinwen/2023－02/27/.content_5743484.htm.
28 张麒麟，叶继元. 论当代图书馆的地位挑战与价值重申——以“知识付费”的兴起与局限为参照［J］. 图书情报工作，2019，63（14）：5－12.
29 陈梁，罗敏，袁润. 专利趋势分析视角的高校技术创新能力比较研究［J］. 图书情报研究，2023，16（1）：114－123.
30 朝乐门. 信息资源管理理论的继承与创新：大数据与数据科学视角［J］. 中国图书馆学报，2019，45（2）：26－42.
31 只莹莹. 元宇宙图书馆：可期的另类文明空间［J］. 图书馆理论与实践，2022（6）：71－76，84.

（上接第 96 页）

络架构正从封闭走向开放，基于封闭网络的网络安全手段已无法适应新时代网络安全形势[9]。湖北省中医医院应抓牢网络安全技术应用和网络安全制度建设两条主线，积极主动实施信息系统网络安全等级保护测评，以评促建，以评促改，评建结合，将网络安全工作制度化、规范化、常态化，有针对性地开展医院核心业务系统应急演练，同时做好数据灾备，齐心共筑医院网络和数据安全防线。

利益声明：所有作者均声明不存在利益冲突。

参考文献

1 中国医院协会信息专业委员会. CHIMA 发布：2021—2022 年度中国医院信息化状况调查报告［EB/OL］.［2023－02－22］. https：//chima.org.cn/Html/News/Articles/16012.html.
2 任子健，沈绍武，肖勇. 中医医院网络安全建设现状分析与思考［J］. 医学信息学杂志，2021，42（8）：42－48.
3 何伟. 基于网络安全等级保护 2.0 的医院综合网络防护探究［J］. 网络安全技术与应用，2020（9）：109－111.
4 王延昭，张晓祥，奈存剑，等. 医院信息系统分级授权管理机制的研究和设计［J］. 中国医院管理，2016，36（3）：54－55.
5 侯爽，李寅，许扬. 基于等保 2.0 标准的互联网医疗系统三级等保测评实践探索［J］. 中国数字医学，2022，17（3）：101－104.
6 孟晓阳，王辰超，朱卫国. 医院网络安全防护策略实践与探讨［J］. 中国卫生信息管理杂志，2020，17（3）：290－295.
7 王磊，魏晓艳，郎爽，等. 医院信息安全等级保护三级评测的应用与实践［J］. 中国数字医学，2015，10（2）：81－83.
8 丁万夫，梁鑫，汤学民，等. 大型综合三甲医院容灾数据中心的研究与应用［J］. 现代信息科技，2022，6（22）：89－92.
9 韦力，段沁，刘志伟. 互联网时代医院网络安全管理综述［J］. 信息网络安全，2019（12）：88－92.